Network Science And Cybersecurity Advances In Inf

If you ally craving such a referred **Network Science And Cybersecurity Advances In Inf** ebook that will meet the expense of you worth, get the very best seller from us currently from several preferred authors. If you want to hilarious books, lots of novels, tale, jokes, and more fictions collections are furthermore launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every books collections Network Science And Cybersecurity Advances In Inf that we will unquestionably offer. It is not regarding the costs. Its practically what you compulsion currently. This Network Science And Cybersecurity Advances In Inf , as one of the most working sellers here will totally be among the best options to review.

Advances in Computer Science for Engineering and Education II - Zhengbing Hu 2019-03-28
This book gathers high-quality, peer-reviewed research papers presented at the Second International Conference on Computer Science, Engineering and Education Applications (ICCSEEA2019), held in Kiev, Ukraine on 26–27 January 2019, and jointly organized by the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" and the International Research Association of Modern Education and Computer Science. The papers discuss state-of-the-art topics and advances in computer science; neural networks; pattern recognition; engineering techniques; genetic coding systems; deep learning and its medical applications; and knowledge representation and its applications in education. Given its scope, the book offers an excellent resource for researchers, engineers, management practitioners, and graduate and undergraduate students interested in computer science and its applications in engineering and education.

Advanced Smart Computing Technologies in Cybersecurity and Forensics - Keshav Kaushik 2021-12-16
This book addresses the topics related to artificial intelligence, the Internet of Things, blockchain technology, and machine learning. It brings together researchers, developers, practitioners, and users interested in cybersecurity and forensics. The first objective is to learn and understand the need for and impact of advanced cybersecurity and forensics and its implementation with multiple smart computational technologies. This objective answers why and how cybersecurity and forensics have evolved as one of the most promising and widely-accepted technologies globally and has widely-accepted applications. The second objective is to learn how to use advanced cybersecurity and forensics practices to answer computational problems where confidentiality, integrity, and availability are essential aspects to handle and answer. This book is structured in such a way so that the field of study is relevant to each reader's major or interests. It aims to help each reader see the relevance of cybersecurity and forensics to their career or interests. This book intends to encourage researchers to develop novel theories to enrich their scholarly knowledge to achieve sustainable development and foster sustainability. Readers will gain valuable knowledge and insights about smart computing technologies using this exciting book. This book: • Includes detailed applications of cybersecurity and forensics for real-life problems • Addresses the challenges and solutions related to implementing cybersecurity in multiple domains of smart computational technologies • Includes the latest trends and areas of research in cybersecurity and forensics • Offers both quantitative and qualitative assessments of the topics Includes case studies that will be helpful for the researchers Prof. Keshav Kaushik is Assistant Professor in the Department of Systemics, School of Computer Science at the University of Petroleum and Energy Studies, Dehradun, India. Dr. Shubham Tayal is Assistant Professor at SR University, Warangal, India. Dr. Akashdeep Bhardwaj is Professor (Cyber Security & Digital Forensics) at the University of Petroleum & Energy Studies (UPES), Dehradun, India. Dr. Manoj Kumar is Assistant Professor (SG) (SoCS) at the University of Petroleum and Energy Studies, Dehradun, India.

Methods, Implementation, and Application of Cyber Security Intelligence and Analytics - Om Prakash, Jena 2022-06-17
Cyber security is a key focus in the modern world as more private information is stored and saved online. In order to ensure vital information is protected from various cyber threats, it is essential to develop a thorough understanding of technologies that can address cyber security challenges. Artificial intelligence has been recognized as an important technology that can be employed successfully in the cyber security sector. Due to this, further study on the potential uses of artificial intelligence is required. Methods, Implementation, and Application of Cyber Security Intelligence and Analytics discusses critical artificial intelligence technologies that are utilized in cyber security and considers various cyber security issues and their optimal solutions supported by artificial intelligence. Covering a range of topics such as malware, smart grid, data breachers, and machine learning, this major reference work is ideal for security analysts, cyber security specialists, data analysts, security professionals, computer scientists, government officials, researchers, scholars, academicians, practitioners, instructors, and students.

Advances in Digital Forensics XVI - Gilbert Peterson 2020-09-06
Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Computer networks, cloud computing, smartphones, embedded devices and the Internet of Things have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence in legal proceedings. Digital forensics also has myriad intelligence applications; furthermore, it has a vital role in cyber security -- investigations of security breaches yield valuable information that can be used to design more secure and resilient systems. Advances in Digital Forensics XVI describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: themes and issues, forensic techniques, filesystem forensics, cloud forensics, social media forensics, multimedia forensics, and novel applications. This book is the sixteenth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of sixteen edited papers from the Sixteenth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India, in the winter of 2020. Advances in Digital Forensics XVI is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities.

Handbook of Research on 5G Networks and Advancements in Computing, Electronics, and Electrical Engineering - Nwajana, Augustine O. 2021-06-25
The advent of the emerging fifth generation (5G) networks has changed the paradigm of how computing, electronics, and electrical (CEE) systems are interconnected. CEE devices and systems, with the help of the 5G technology, can now be seamlessly linked in a way that is rapidly turning the globe into a digital world. Smart cities and internet of things have come to stay but not without some challenges, which must be discussed. The Handbook of Research on 5G Networks and Advancements in Computing, Electronics, and Electrical Engineering focuses on current technological innovations as the world rapidly heads towards becoming a global smart city. It covers important topics such as power systems, electrical engineering, mobile communications, network, security, and more. This book examines vast types of technologies and their roles in society with a focus on how each works, the impacts it has, and the future for developing a global smart city. This book is ideal for both industrial and academic researchers, scientists, engineers, educators, practitioners, developers, policymakers, scholars, and students interested in 5G technology and the future of engineering, computing, and technology in human society.

Advanced Digital Image Steganography Using LSB, PVD, and EMD: Emerging Research and Opportunities - Swain, Gandharba 2019-06-28
In the last few decades, the use of the Internet has grown tremendously,

and the use of online communications has grown even more. The lack of security in private messages between individuals, however, allows hackers to collect loads of sensitive information. Modern security measures are required to prevent this attack on the world s communication technologies. Advanced Digital Image Steganography Using LSB, PVD, and EMD: Emerging Research and Opportunities provides evolving research exploring the theoretical and practical aspects of data encryption techniques and applications within computer science. The book provides introductory knowledge on steganography and its importance, detailed analysis of how RS and PDH are performed, discussion on pixel value differencing principles, and hybrid approaches using substitution, PVD, and EMD principles. It is ideally designed for researchers and graduate and under graduate students seeking current research on the security of data during transit.

Advances in Malware and Data-Driven Network Security - Brij Gupta 2021

"This book describes some of the recent notable advances in threat-detection using machine-learning and artificial-intelligence with a focus on malwares, covering the current trends in ML/statistical approaches to detecting, clustering or classification of cyber-threats extensively"--

Advanced Computing, Networking and Security - P. Santhi Thilagam 2012-04-20

This book constitutes revised selected papers from the International Conference on Advanced Computing, Networking and Security, ADCONS 2011, held in Surathkal, India, in December 2011. The 73 papers included in this book were carefully reviewed and selected from 289 submissions. The papers are organized in topical sections on distributed computing, image processing, pattern recognition, applied algorithms, wireless networking, sensor networks, network infrastructure, cryptography, Web security, and application security.

Advances in Computer, Communication and Computational Sciences - Sanjiv K. Bhatia 2020-11-28

This book discusses recent advances in computer and computational sciences from upcoming researchers and leading academics around the globe. It presents high-quality, peer-reviewed papers presented at the International Conference on Computer, Communication and Computational Sciences (IC4S 2019), which was held on 11—12 October 2019 in Bangkok. Covering a broad range of topics, including intelligent hardware and software design, advanced communications, intelligent computing techniques, intelligent image processing, the Web and informatics, it offers readers from the computer industry and academia key insights into how the advances in next-generation computer and communication technologies can be shaped into real-life applications.

Advances in Internet, Data and Web Technologies - Leonard Barolli 2020-01-30

This book presents original contributions on the theories and practices of emerging Internet, data and web technologies and their applicability in businesses, engineering and academia. The Internet has become the most proliferative platform for emerging large-scale computing paradigms. Among them, data and web technologies are two most prominent paradigms, and manifest in a variety of forms such as data centers, cloud computing, mobile cloud, mobile web services and so on. Together, these technologies form a digital ecosystem based on the data cycle, from capturing to processing, analysis and visualization. The investigation of various research and development issues in this digital ecosystem is made all the more important by the ever-increasing needs of real-life applications, which involve storing and processing large amounts of data. As a key feature, the book addresses advances in the life-cycle exploitation of data generated from the digital ecosystem, and data technologies that create value for businesses, moving toward a collective intelligence approach. Given its scope, the book offers a valuable reference guide for researchers, software developers, practitioners and students interested in the field of data and web technologies.

Advanced Soft Computing Techniques in Data Science, IoT and Cloud Computing - Sujata Dash 2021-11-05

This book plays a significant role in improvising human life to a great extent. The new applications of soft computing can be regarded as an emerging field in computer science, automatic control engineering, medicine, biology application, natural environmental engineering, and pattern recognition. Now, the exemplar model for soft computing is human brain. The use of various techniques of soft computing is nowadays successfully implemented in many domestic, commercial, and industrial applications due to the low-cost and very high-performance digital processors and also the decline price of the memory chips. This is the main reason behind the wider expansion of soft computing techniques and its application areas. These computing methods also play a significant role in the design and optimization in diverse engineering disciplines. With the influence and the development of the Internet of things (IoT) concept, the need for using soft computing techniques has become more significant than ever. In general, soft computing methods are closely similar to biological processes than traditional techniques, which are mostly based on formal logical systems, such as sentential logic and predicate logic, or rely heavily on computer-aided numerical analysis. Soft computing techniques are anticipated to complement each other. The aim of these techniques is to accept imprecision, uncertainties, and approximations to get a rapid solution. However, recent advancements in representation soft computing algorithms (fuzzy logic,evolutionary computation, machine learning, and probabilistic reasoning) generate a more intelligent and robust system providing a human interpretable, low-cost, approximate solution. Soft computing-based algorithms have demonstrated great performance to a variety of areas including multimedia retrieval, fault tolerance, system modelling, network architecture, Web semantics, big data analytics, time series, biomedical and health informatics, etc. Soft computing approaches such as genetic programming (GP), support vector machine–firefly algorithm (SVM-FFA), artificial neural network (ANN), and support vector machine–wavelet (SVM–Wavelet) have emerged as powerful computational models. These have also shown significant success in dealing with massive data analysis for large number of applications. All the researchers and practitioners will be highly benefited those who are working in field of computer engineering, medicine, biology application, signal processing, and mechanical engineering. This book is a good collection of state-of-the-art approaches for soft computing-based applications to various engineering fields. It is very beneficial for the new researchers and practitioners working in the field to quickly know the best performing methods. They would be able to compare different approaches and can carry forward their research in the most important area of research which has direct impact on betterment of the human life and health. This book is very useful because there is no book in the market which provides a good collection of state-of-the-art methods of soft computing-based models for multimedia retrieval, fault tolerance, system modelling, network architecture, Web semantics, big data analytics, time series, and biomedical and health informatics.

Advanced Practical Approaches to Web Mining Techniques and Application - Obaid, Ahmed J. 2022-03-18

The rapid increase of web pages has introduced new challenges for many organizations as they attempt to extract information from a massive corpus of web pages. Finding relevant information, eliminating irregular content, and retrieving accurate results has become extremely difficult in today’s world where there is a surplus of information available. It is crucial to further understand and study web mining in order to discover the best ways to connect users with appropriate information in a timely manner. Advanced Practical Approaches to Web Mining Techniques and Application aims to illustrate all the concepts of web mining and fosters transformative, multidisciplinary, and novel approaches that introduce the practical method of analyzing various web data sources and extracting knowledge by taking into consideration the unique challenges present in the environment. Covering a range of topics such as data science and security threats, this reference work is ideal for industry professionals, researchers, academicians, practitioners, scholars, instructors, and students.

Handbook of Advanced Performability Engineering - Krishna B. Misra 2020-11-16

This book considers all aspects of performability engineering, providing a holistic view of the activities associated with a product throughout its entire life cycle of the product, as well as the cost of minimizing the environmental impact at each stage, while maximizing the performance. Building on the editor's previous Handbook of Performability Engineering, it explains how performability engineering provides us with a framework to consider both dependability and sustainability in the optimal design of products, systems and services, and explores the role of performability in energy and waste minimization, raw material selection, increased production volume, and many other areas of engineering and production. The book discusses a range of new ideas, concepts, disciplines, and applications in performability, including smart manufacturing and Industry 4.0; cyber-physical systems and artificial intelligence; digital transformation of railways; and asset management. Given its broad scope, it will appeal to researchers, academics, industrial practitioners and postgraduate students involved in manufacturing, engineering, and system and product development.

Social Media in India - Francis P. Barclay 2021-11-29

Social media is acutely prone to misuse—thanks to its independent and undisciplined nature—necessitating regulation. The book addresses this concern, analysing critical sociopolitical issues related to social media regulation and discussing the latest developments in India. Social Media in India: Regulatory Needs, Issues and Challenges reviews the values of freedom of expression, privacy and regulation, and proposes strategies to balance the triad, aiding policy formation, at a time when the Indian government and significant social media intermediaries are in a standoff over the newly ordained IT rules. This book covers all aspects that need to be examined for the overhaul of the regulatory framework including addiction, awareness, rampant misinformation, political applications and conflicts. Highlighting such social and user-centric challenges to the sustainability of online social networks, the book argues for the need of a robust regulatory framework and advocates an attitude adjustment about privacy and social media in the age of disinformation.

Advances in Human Factors in Cybersecurity - Tareq Z. Ahram 2018-06-23

This book reports on the latest research and developments in the field of cybersecurity, particularly focusing on personal security and new methods for reducing human error and increasing cyber awareness, as well as innovative solutions for increasing the security of advanced Information Technology (IT) infrastructures. It covers a broad range of topics, including methods for human training; novel cyber-physical and process-control systems; social, economic, and behavioral aspects of cyberspace; issues concerning the cybersecurity index; security metrics for enterprises; and risk evaluation. Based on the AHFE 2018 International Conference on Human Factors in Cybersecurity, held on July 21–25, 2018, in Orlando, Florida, USA, the book not only presents innovative cybersecurity technologies, but also discusses emerging threats, current gaps in the available systems, and future challenges that can be successfully overcome with the help of human factors research.

An Interdisciplinary Approach to Modern Network Security - Sabyasachi Pramanik 2022-05-03

An Interdisciplinary Approach to Modern Network Security presents the latest methodologies and trends in detecting and preventing network threats. Investigating the potential of current and emerging security technologies, this publication is an all-inclusive reference source for academicians, researchers, students, professionals, practitioners, network analysts and technology specialists interested in the simulation and application of computer network protection. It presents theoretical frameworks and the latest research findings in network security technologies, while analyzing malicious threats which can compromise network integrity. It discusses the security and optimization of computer networks for use in a variety of disciplines and fields. Touching on such matters as mobile and VPN security, IP spoofing and intrusion detection, this edited collection emboldens the efforts of researchers, academics and network administrators working in both the public and private sectors. This edited compilation includes chapters covering topics such as attacks and countermeasures, mobile wireless networking, intrusion detection systems, next-generation firewalls, web security and much more. Information and communication systems are an essential component of our society, forcing us to become dependent on these infrastructures. At the same time, these systems are undergoing a convergence and interconnection process that has its benefits, but also raises specific threats to user interests. Citizens and organizations must feel safe when using cyberspace facilities in order to benefit from its advantages. This book is interdisciplinary in the sense that it covers a wide range of topics like network security threats, attacks, tools and procedures to mitigate the effects of malware and common network attacks, network security architecture and deep learning methods of intrusion detection.

Essential Cybersecurity Science - Josiah Dykstra 2015-12-08

If you’re involved in cybersecurity as a software developer, forensic investigator, or network administrator, this practical guide shows you how to apply the scientific method when assessing techniques for protecting your information systems. You’ll learn how to conduct scientific experiments on everyday tools and procedures, whether you’re evaluating corporate security systems, testing your own security product, or looking for bugs in a mobile game. Once author Josiah Dykstra gets you up to speed on the scientific method, he helps you focus on standalone, domain-specific topics, such as cryptography, malware analysis, and system security engineering. The latter chapters include practical case studies that demonstrate how to use available tools to conduct domain-specific scientific experiments. Learn the steps necessary to conduct scientific experiments in cybersecurity Explore fuzzing to test how your software handles various inputs Measure the performance of the Snort intrusion detection system Locate malicious “needles in a haystack” in your network and IT environment Evaluate cryptography design and application in IoT products Conduct an experiment to identify relationships between similar malware binaries Understand system-level security requirements for enterprise networks and web services

Computation, Cryptography, and Network Security - Nicholas J. Daras 2015-09-16

Analysis, assessment, and data management are core competencies for operation research analysts. This volume addresses a number of issues and developed methods for improving those skills. It is an outgrowth of a conference held in April 2013 at the Hellenic Military Academy, and brings together a broad variety of mathematical methods and theories with several applications. It discusses directions and pursuits of scientists that pertain to engineering sciences. It is also presents the theoretical background required for algorithms and techniques applied to a large variety of concrete problems. A number of open questions as well as new future areas are also highlighted. This book will appeal to operations research analysts, engineers, community decision makers, academics, the military community, practitioners sharing the current “state-of-the-art,” and analysts from coalition partners. Topics covered include Operations Research, Games and Control Theory, Computational Number Theory and Information Security, Scientific Computing and Applications, Statistical Modeling and Applications, Systems of Monitoring and Spatial Analysis.

Advances in Unconventional Computing - Andrew Adamatzky 2016-07-18

The unconventional computing is a niche for interdisciplinary science, cross-bred of computer science, physics, mathematics, chemistry, electronic engineering, biology, material science and nanotechnology. The aims of this book are to uncover and exploit principles and mechanisms of information processing in and functional properties of physical, chemical and living systems to develop efficient algorithms, design optimal architectures and manufacture working prototypes of future and emergent computing devices. This first volume presents theoretical foundations of the future and emergent computing paradigms and architectures. The topics covered are computability, (non-)universality and complexity of computation; physics of computation, analog and quantum computing; reversible and asynchronous devices; cellular automata and other mathematical machines; P-systems and cellular computing; infinity and spatial computation; chemical and reservoir computing. The book is the encyclopedia, the first ever complete authoritative account, of the theoretical and experimental findings in the unconventional computing written by the world leaders in the field. All chapters are self-contains, no specialist background is required to appreciate ideas, findings, constructs and designs presented. This treatise in unconventional computing appeals to readers from all walks of life, from high-school pupils to university professors, from mathematicians, computers scientists and engineers to chemists and biologists.

Cyber Security - M. U. Bokhari 2018-04-27

This book comprises select proceedings of the annual convention of the Computer Society of India. Divided into 10 topical volumes, the proceedings present papers on state-of-the-art research, surveys, and succinct reviews. The volume covers diverse topics ranging from information security to cryptography and from encryption to intrusion detection. This book focuses on Cyber Security. It aims at informing the readers about the technology in general and the internet in particular. The book uncovers the various nuances of information security, cyber security and its various dimensions. This book also covers latest security trends, ways to combat cyber threats including the detection and mitigation of security threats and risks. The contents of this book will prove useful to professionals and researchers alike.

Advances in Human Factors in Cybersecurity - Denise Nicholson 2016-08-16

This book reports on the latest research and developments in the field of cybersecurity, giving a special emphasis on personal security and new methods for reducing human error and increasing cyber awareness, and innovative solutions for increasing the security of advanced Information Technology (IT) infrastructures. It covers a wealth of topics, including methods for human training, novel Cyber-Physical and Process-Control Systems, social, economic and behavioral aspects of the cyberspace, issues concerning the cyber security index, security metrics for enterprises, risk evaluation, and many others. Based on the AHFE 2016 International Conference on Human Factors in Cybersecurity, held on July 27-31, 2016, in Walt Disney World®, Florida, USA, this book not only presents innovative cybersecurity technologies, but also discusses emerging threats, current gaps in the available systems and future challenges that may be coped with through the help of human factors research.

Cybersecurity Data Science - Scott Mongeau 2021-10-01
This book encompasses a systematic exploration of Cybersecurity Data Science (CSDS) as an emerging profession, focusing on current versus idealized practice. This book also analyzes challenges facing the emerging CSDS profession, diagnoses key gaps, and prescribes treatments to facilitate advancement. Grounded in the management of information systems (MIS) discipline, insights derive from literature analysis and interviews with 50 global CSDS practitioners. CSDS as a diagnostic process grounded in the scientific method is emphasized throughout Cybersecurity Data Science (CSDS) is a rapidly evolving discipline which applies data science methods to cybersecurity challenges. CSDS reflects the rising interest in applying data-focused statistical, analytical, and machine learning-driven methods to address growing security gaps. This book offers a systematic assessment of the developing domain. Advocacy is provided to strengthen professional rigor and best practices in the emerging CSDS profession. This book will be of interest to a range of professionals associated with cybersecurity and data science, spanning practitioner, commercial, public sector, and academic domains. Best practices framed will be of interest to CSDS practitioners, security professionals, risk management stewards, and institutional stakeholders. Organizational and industry perspectives will be of interest to cybersecurity analysts, managers, planners, strategists, and regulators. Research professionals and academics are presented with a systematic analysis of the CSDS field, including an overview of the state of the art, a structured evaluation of key challenges, recommended best practices, and an extensive bibliography.

Advances in Smart Grid Power System - Anuradha Tomar 2020-10-23
Advances in Smart Grid Power System: Network, Control and Security discusses real world problems, solutions, and best practices in related fields. The book includes executable plans for smart grid systems, their network communications, tactics on protecting information, and response plans for cyber incidents. Moreover, it enables researchers and energy professionals to understand the future of energy delivery systems and security. Covering fundamental theory, mathematical formulations, practical implementations, and experimental testing procedures, this book gives readers invaluable insights into the field of power systems, their quality and reliability, their impact, and their importance in cybersecurity. Includes supporting illustrations and tables along with valuable end of chapter reference sets Provides a working guideline for the design and analysis of smart grids and their applications Features experimental testing procedures in smart grid power systems, communication networks, reliability, and cybersecurity

Artificial Intelligence and Cybersecurity - Ishaani Priyadarshini 2022-02-04
Artificial intelligence and cybersecurity are two emerging fields that have made phenomenal contributions toward technological advancement. As cyber-attacks increase, there is a need to identify threats and thwart attacks. This book incorporates recent developments that artificial intelligence brings to the cybersecurity world. Artificial Intelligence and Cybersecurity: Advances and Innovations provides advanced system implementation for Smart Cities using artificial intelligence. It addresses the complete functional framework workflow and explores basic and high-level concepts. The book is based on the latest technologies covering major challenges, issues and advances, and discusses intelligent data management and automated systems. This edited book provides a premier interdisciplinary platform for researchers, practitioners and educators. It presents and discusses the most recent innovations, trends and concerns as well as practical challenges and solutions adopted in the fields of artificial intelligence and cybersecurity.

Network Science and Cybersecurity - Robinson E. Pino 2013-06-14
Network Science and Cybersecurity introduces new research and development efforts for cybersecurity solutions and applications taking place within various U.S. Government Departments of Defense, industry and academic laboratories. This book examines new algorithms and tools, technology platforms and reconfigurable technologies for cybersecurity systems. Anomaly-based intrusion detection systems (IDS) are explored as a key component of any general network intrusion detection service, complementing signature-based IDS components by attempting to identify novel attacks. These attacks may not yet be known or have well-developed signatures. Methods are also suggested to simplify the construction of metrics in such a manner that they retain their ability to effectively cluster data, while simultaneously easing human interpretation of outliers. This is a professional book for practitioners or government employees working in cybersecurity, and can also be used as a reference. Advanced-level students in computer science or electrical engineering studying security will also find this book useful .

Advances in Nature-Inspired Cyber Security and Resilience - Shishir Kumar Shandilya 2022
This book presents a comprehensive reference source for dynamic and innovative research in the field of cyber security, focusing on nature-inspired research and applications. The authors present the design and development of future-ready cyber security measures, providing a critical and descriptive examination of all facets of cyber security with a special focus on recent technologies and applications. The book showcases the advanced defensive cyber security mechanism that is a requirement in the industry and highlights measures that provide efficient and fast solutions. The authors explore the potential of AI-based and nature-inspired based computing compatibilities in establishing an adaptive defense mechanism system. The book focuses on current research while highlighting the empirical results along with theoretical concepts to provide a reference for students, researchers, scholars, professionals, and practitioners in the field of cyber security and analytics. This book features contributions from leading scholars from all over the world. Presents a comprehensive reference for innovative research in the field of cyber security and resilience with a nature-inspired focus; Presents research in artificial intelligence, machine learning, soft computing, and nature-inspired computing that can advance real-time cyber security applications; Relevant to industry professionals and researchers in cyber-security.

Advances in Cybersecurity Management - Kevin Daimi 2021-06-15
This book concentrates on a wide range of advances related to IT cybersecurity management. The topics covered in this book include, among others, management techniques in security, IT risk management, the impact of technologies and techniques on security management, regulatory techniques and issues, surveillance technologies, security policies, security for protocol management, location management, GOS management, resource management, channel management, and mobility management. The authors also discuss digital contents copyright protection, system security management, network security management, security management in network equipment, storage area networks (SAN) management, information security management, government security policy, web penetration testing, security operations, and vulnerabilities management. The authors introduce the concepts, techniques, methods, approaches and trends needed by cybersecurity management specialists and educators for keeping current their cybersecurity management knowledge. Further, they provide a glimpse of future directions where cybersecurity management techniques, policies, applications, and theories are headed. The book is a rich collection of carefully selected and reviewed manuscripts written by diverse cybersecurity management experts in the listed fields and edited by prominent cybersecurity management researchers and specialists.

Cyber Security and Network Security - Sabyasachi Pramanik 2022-04-19
CYBER SECURITY AND NETWORK SECURITY Written and edited by a team of experts in the field, this is the most comprehensive and up-to-date study of the practical applications of cyber security and network security for engineers, scientists, students, and other professionals. Digital assaults are quickly becoming one of the most predominant issues on the planet. As digital wrongdoing keeps on expanding, it is increasingly more important to investigate new methodologies and advances that help guarantee the security of online networks. Ongoing advances and innovations have made great advances for taking care of security issues in a methodical manner. In light of this, organized security innovations have been delivered so as to guarantee the security of programming and correspondence functionalities at fundamental, improved, and engineering levels. This outstanding new volume covers all of the latest advances, innovations, and developments in practical applications for cybersecurity and network security. This team of editors represents some of the most well-known and respected experts in the area, creating this comprehensive, up-to-date coverage of the issues of the day and state of the art. Whether for the veteran engineer or

scientist or a student, this volume is a must-have for any library.

Handbook of Research on Machine and Deep Learning Applications for Cyber Security - Ganapathi, Padmavathi 2019-07-26

As the advancement of technology continues, cyber security continues to play a significant role in today␣s world. With society becoming more dependent on the internet, new opportunities for virtual attacks can lead to the exposure of critical information. Machine and deep learning techniques to prevent this exposure of information are being applied to address mounting concerns in computer security. The Handbook of Research on Machine and Deep Learning Applications for Cyber Security is a pivotal reference source that provides vital research on the application of machine learning techniques for network security research. While highlighting topics such as web security, malware detection, and secure information sharing, this publication explores recent research findings in the area of electronic security as well as challenges and countermeasures in cyber security research. It is ideally designed for software engineers, IT specialists, cybersecurity analysts, industrial experts, academicians, researchers, and post-graduate students.

Advanced Network Technologies and Intelligent Computing - Isaac Woungang 2022

This volume constitutes the selected papers presented at the First International Conference on Advanced Network Technologies and Intelligent Computing, ANTIC 2021, hed in Varanasi, India, in December 2021. Due to the COVID-19 pandemic the conference was held online. The 61 papers presented were thoroughly reviewed and selected from 593 submissions. They are organized in topical sections on advanced network technologies and intelligent computing.

Advances in Malware and Data-Driven Network Security - Gupta, Brij B. 2021-11-12

Every day approximately three-hundred thousand to four-hundred thousand new malware are registered, many of them being adware and variants of previously known malware. Anti-virus companies and researchers cannot deal with such a deluge of malware – to analyze and build patches. The only way to scale the efforts is to build algorithms to enable machines to analyze malware and classify and cluster them to such a level of granularity that it will enable humans (or machines) to gain critical insights about them and build solutions that are specific enough to detect and thwart existing malware and generic-enough to thwart future variants. Advances in Malware and Data-Driven Network Security comprehensively covers data-driven malware security with an emphasis on using statistical, machine learning, and AI as well as the current trends in ML/statistical approaches to detecting, clustering, and classification of cyber-threats. Providing information on advances in malware and data-driven network security as well as future research directions, it is ideal for graduate students, academicians, faculty members, scientists, software developers, security analysts, computer engineers, programmers, IT specialists, and researchers who are seeking to learn and carry out research in the area of malware and data-driven network security.

Advances in Cyber Security - Mohammed Anbar 2021-02-04

This book presents refereed proceedings of the Second International Conference on Advances in Cyber Security, ACeS 2020, held in Penang, Malaysia, in September 2020. Due to the COVID-19 pandemic the conference was held online. The 46 full papers and 1 short paper were carefully reviewed and selected from 132 submissions. The papers are organized in topical sections on internet of things, industry 4.0 and blockchain, and cryptology; digital forensics and surveillance, botnet and malware, and intrusion detection/prevention; ambient cloud and edge computing, wireless and cellular communication; governance, social media, mobile and web, data privacy, data policy and fake news.

At the Nexus of Cybersecurity and Public Policy - National Research Council 2014-06-16

We depend on information and information technology (IT) to make many of our day-to-day tasks easier and more convenient. Computers play key roles in transportation, health care, banking, and energy. Businesses use IT for payroll and accounting, inventory and sales, and research and development. Modern military forces use weapons that are increasingly coordinated through computer-based networks. Cybersecurity is vital to protecting all of these functions. Cyberspace is vulnerable to a broad spectrum of hackers, criminals, terrorists, and state actors. Working in cyberspace, these malevolent actors can steal money, intellectual property, or classified information; impersonate law-abiding parties for their own purposes; damage important data; or deny the availability of normally accessible services. Cybersecurity issues arise because of three factors taken together - the presence of malevolent actors in cyberspace, societal reliance on IT for many important functions, and the presence of vulnerabilities in IT systems. What steps can policy makers take to protect our government, businesses, and the public from those would take advantage of system vulnerabilities? At the Nexus of Cybersecurity and Public Policy offers a wealth of information on practical measures, technical and nontechnical challenges, and potential policy responses. According to this report, cybersecurity is a never-ending battle; threats will evolve as adversaries adopt new tools and techniques to compromise security. Cybersecurity is therefore an ongoing process that needs to evolve as new threats are identified. At the Nexus of Cybersecurity and Public Policy is a call for action to make cybersecurity a public safety priority. For a number of years, the cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the fundamentals of cybersecurity and the discussion of potential policy responses, this book will be a resource for policy makers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace.

Cybersecurity in the Electricity Sector - Rafał Leszczyna 2019-08-30

This book offers a systematic explanation of cybersecurity protection of electricity supply facilities, including discussion of related costs, relevant standards, and recent solutions. The author explains the current state of cybersecurity in the electricity market, and cybersecurity standards that apply in that sector. He then offers a systematic approach to cybersecurity management, including new methods of cybersecurity assessment, cost evaluation and comprehensive defence. This monograph is suitable for practitioners, professionals, and researchers engaged in critical infrastructure protection.

Advances in Network-Based Information Systems - Leonard Barolli 2017-08-21

This book highlights the latest research findings, innovative research results, methods and development techniques from both theoretical and practical perspectives related to the emerging areas of information networking and their applications. It includes the Proceedings of the 20th International Conference on Network-Based Information Systems (NBiS-2017), held on August 24–26, 2017 in Toronto, Canada. Today's networks and information systems are evolving rapidly. Further, there are dynamic new trends and applications in information networking such as wireless sensor networks, ad hoc networks, peer-to-peer systems, vehicular networks, opportunistic networks, grid and cloud computing, pervasive and ubiquitous computing, multimedia systems, security, multi-agent systems, high-speed networks, and web-based systems. These networks are expected to manage the increasing number of users, provide support for a range of services, guarantee the quality of service (QoS), and optimize their network resources. In turn, these demands are the source of various research issues and challenges that have to be overcome – and which these Proceeding address.

Advanced Concepts, Methods, and Applications in Semantic Computing - Daramola, Olawande 2020-12-18

Semantic computing is critical for the development of semantic systems and applications that must utilize semantic analysis, semantic description, semantic interfaces, and semantic integration of data and services to deliver their objectives. Semantic computing has enormous capabilities to enhance the efficiency and throughput of systems that are based on key emerging concepts and technologies such as semantic web, internet of things, blockchain technology, and knowledge graphs. Thus, research that expounds advanced concepts, methods, technologies, and applications of semantic computing for solving challenges in real-world domains is vital. Advanced Concepts, Methods, and Applications in Semantic Computing is a scholarly reference book that provides a sound theoretical foundation for the application of semantic methods, concepts, and technologies for practical problem solving. It is designed as a comprehensive and reliable resource on how semantic-oriented approaches can be used to aid new emergent technologies and tackle real-world problems. Covering topics that include deep learning, machine learning, blockchain technology, and semantic web services, this book is ideal for professionals, academicians, researchers, and students working in the field of semantic computing in various disciplines, including but not limited to software engineering, systems engineering, knowledge engineering, electronic commerce, computer science, and information technology.

Advances in Computing, Informatics, Networking and Cybersecurity - Petros Nicopolitidis 2022

This book presents new research contributions in the above-mentioned fields. Information and communication technologies (ICT) have an integral role in todays society. Four major driving pillars in the field are computing, which nowadays enables data processing in unprecedented speeds, informatics, which derives information stemming for processed data to feed relevant applications, networking, which interconnects the various computing infrastructures and cybersecurity for addressing the growing concern for secure and lawful use of the ICT infrastructure and services. Its intended readership covers senior undergraduate and graduate students in Computer Science and Engineering and Electrical Engineering, as well as researchers, scientists, engineers, ICT managers, working in the relevant fields and industries.

Cybersecurity and Secure Information Systems - Aboul Ella Hassanien 2019-06-19

This book provides a concise overview of the current state of the art in cybersecurity and shares novel and exciting ideas and techniques, along with specific cases demonstrating their practical application. It gathers contributions by both academic and industrial researchers, covering all aspects of cybersecurity and addressing issues in secure information systems as well as other emerging areas. The content comprises high-quality research articles and reviews that promote a multidisciplinary approach and reflect the latest advances, challenges, requirements and methodologies. Thus, the book investigates e.g. security vulnerabilities, cybercrime, and privacy issues related to big data analysis, as well as advances in digital forensics, secure smart city services, and risk mitigation strategies for devices employing cyber-physical systems. Given its scope, the book offers a valuable resource for students, researchers, IT professionals and providers, citizens, consumers and policymakers involved or interested in the modern security procedures needed to protect our information and communication resources. Its goal is to foster a community committed to further research and education, and one that can also translate its findings into concrete practices.

Advances in Security, Networks, and Internet of Things - Kevin Daimi 2021-07-10

The book presents the proceedings of four conferences: The 19th International Conference on Security & Management (SAM'20), The 19th International Conference on Wireless Networks (ICWN'20), The 21st International Conference on Internet Computing & Internet of Things (ICOMP'20), and The 18th International Conference on Embedded Systems, Cyber-physical Systems (ESCS'20). The conferences took place in Las Vegas, NV, USA, July 27-30, 2020. The conferences are part of the larger 2020 World Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE'20), which features 20 major tracks. Authors include academics, researchers, professionals, and students. Presents the proceedings of four conferences as part of the 2020 World Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE'20); Includes the tracks on security & management, wireless networks, internet computing and IoT, and embedded systems as well as cyber-physical systems; Features papers from SAM’20, ICWN’20, ICOMP’20 and ESCS’20.

Advances in Computer Science for Engineering and Education III - Zhengbing Hu 2020-08-05

This book comprises high-quality refereed research papers presented at the Third International Conference on Computer Science, Engineering and Education Applications (ICCSEEA2020), held in Kyiv, Ukraine, on 21–22 January 2020, organized jointly by National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, National Aviation University, and the International Research Association of Modern Education and Computer Science. The topics discussed in the book include state-of-the-art papers in computer science, artificial intelligence, engineering techniques, genetic coding systems, deep learning with its medical applications, and knowledge representation with its applications in education. It is an excellent source of references for researchers, graduate students, engineers, management practitioners, and undergraduate students interested in computer science and their applications in engineering and education.